PathScan: Finding the Attacker Within the Network

LA-UR-13-29444

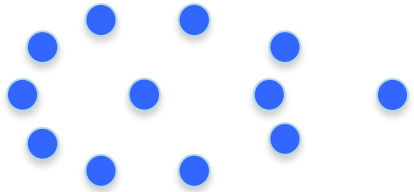
PathScan: Finding the Attacker Within the Network

Los Alamos NATIONAL LABORATORY EST. 1943

PathScan Analyzes the Behavior of Subgraphs of Communicating Computers for Anomaly Detection

LDRD innovation for our nation

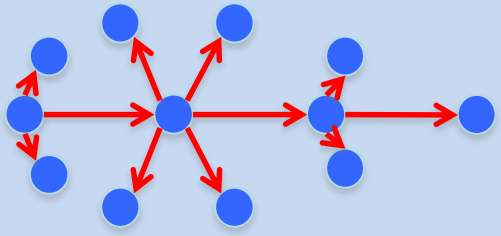
BACKGROUND & MOTIVATION



Modern Anomaly Detection for Computer Networks Models Events Independently

- Identifying deviations from historic activity
- Does not ask about deviations among subgraphs of communicating hosts

INNOVATION



Analyzing subgraphs of communicating computers provides better signal-to-noise ratios.

- Lower false alarm rate
- Higher true alarm rate
- Better forensic information—providing a fuller description of the overall attack

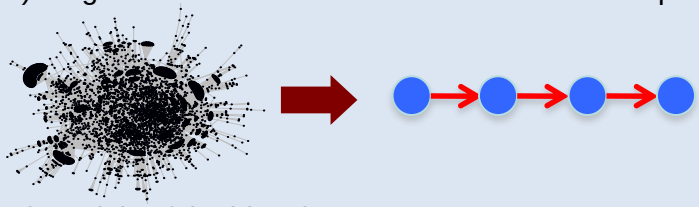
DESCRIPTION

Detecting Advanced Persistent Threats (APTs) on operational networks in near real-time

- Statistical modeling of network behavior
- Fast, parallel subgraph enumeration,
- Examining billions of subgraphs within enterprise-level computer networks

How it works:

1) Large networks are broken into billions of small paths



2) Models of the historic behavior are compared with observed data on each path

$$\lambda_\gamma = -2\log\left(\frac{\mathcal{L}\left(\hat{\theta}(\gamma);\mathbf{X}(\gamma)\right)}{\sup_{\theta\in\Theta}\mathcal{L}(\theta(\gamma);\mathbf{X}(\gamma))}\right)$$

3) Those paths which exceed a threshold of anomalousness (weirdness) are alarmed upon

Assumptions & Limitations

- Main limitation is often access to high-quality internal network data
- We provide expertise in collecting data to help new networks quickly get up to speed

TRL 5: PathScan is being tested in an operational testbed at LANL on LANL's networks. PathScan has also been tested on other Government networks

ANTICIPATED IMPACT

Real-time detection of sophisticated adversaries traversal behavior on a network

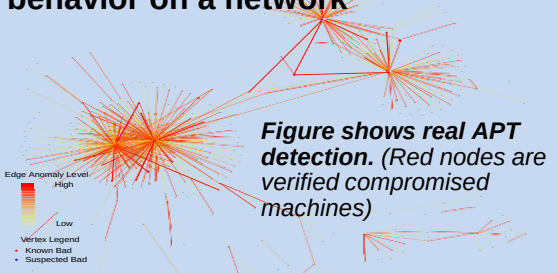


Figure shows real APT detection. *(Red nodes are verified compromised machines)*

Deep analysis of historical network data to find previously unknown attackers

PATH FORWARD

Implement outside LANL:

Prototype and beta test on external networks:

- Government and commercial

Validate and harden algorithms against broader sets of network data:

- Other Government
- Commercial: Financial industry, Oil & gas industry. entertainment industry, etc.

Potential End Users:

- All large IT networks (government and commercial) at enterprise level

Point of Contact: Mike Fisk
Advanced Computing Solutions Program Office
505-667-5119, mfisk@lanl.gov